REMARKS

Claims 1, 4-14, and 16-36 were previously pending in this application. In this response, claims 1, 4-10, 12-13, 28, and 33 are amended. Claims 11 and 25 are canceled. Claims 1, 4-10, 12-14, 16-24, and 26-36 remain pending.

37 CFR 1.75(c) OBJECTIONS

Claims 11 and 25 are objected to as being of improper dependent form. Applicant has canceled claims 11 and 25, thereby rendering these objections moot.

35 U.S.C. § 102 and 35 U.S.C. § 103 REJECTIONS

Claims 1, 4-6, 8-14, 16, 18-28, 31, and 33-36 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,636,838 to Perlman et al. (hereinafter "Perlman"). Claims 7 and 17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of U.S. Patent No. 6,681,327 to Jardin (hereinafter "Jardin"). Claims 29, 30, and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman. The Applicant respectfully traverses these rejections.

As stated in the specification, the presently claimed subject matter is generally concerned with, among other things:

> ... bi-directional multiple hopping via a proxy. The invention has two scenarios, a reverse scenario and a forward scenario, which can also be combined. In the reverse scenario, there is a client, one or more proxies, and an origin, or publishing, server. The term origin, or publishing, server is used to distinguish this server from the proxies,

> which may also be servers. The client sends encrypted data to the proxy over an unsecure network, such as the Internet, in a first hop. The proxy decrypts the encrypted data, and performs an action, or test, relative to the data, such as ensuring that the data does not present a security risk, and offering the benefit of redirecting the traffic as appropriate. Assuming that the data passes this test, the proxy can do one of two things. First, the proxy can send the data over a secure network of which it is a part, such as an intranet or other private network, to an origin server that is also part of the secure network, in a second hop. Second, the proxy can first re-encrypt the data, and send the data either over the secure network or the unsecure network to a server or another proxy, also in a second hop.
>
> Specification, page 3, line 7-20

> In the forward scenario of the invention, there is also a client, a proxy, and an origin server. The client sends unencrypted data to the proxy over a secure network in a first hop. The client may be a thin client, such as a wireless phone or a personal digital assistant (PDA) device, and the secure network may be the wireless or carrier network for the wireless phone. The proxy in the carrier or wireless network performs an action, or test, relative to the unencrypted data, such as ensuring that the unencrypted data is acceptable for transmission. Assuming that the unencrypted data passes this test, the proxy encrypts the unencrypted data into encrypted data, and sends the encrypted data to the origin server over an unsecure network, such as the Internet, in a second hop.
>
> Specification, page 4, line 18 to page 5, line 3

Perlman generally describes mechanisms for performing content screening on messages that are protected by end-to-end encryption. Perlman describes communications between a client and server where the communications are secure - for example, because the communications are encrypted - from the time the communication leaves the client and until it reaches the server. By using techniques described in Perlman, an entity called a content screener may decrypt and examine the content of the communications. In some implementations, such as the implementations described with respect to FIG. 1 in Perlman, the content screener is located "between" the client and the server, so that it "sees" the communication before the communication reaches the server. In other implementations, such as those described with respect to FIG. 6 in Perlman, the content screener is located outside of the path between the client and the server and may, for example, examine the communications only after the communications have reached the server. In some of the implementations described in Perlman, the content screener may be a part of a firewall that protects a "private" network from unwanted traffic outside the private network.

Jardin generally describes a server that brokers secure transactions, including those secured using SSL, for distribution to a plurality of fulfillment servers.

Claim 1

Claim 1, as amended, recites "a method comprising: receiving encrypted data at a proxy from a client over an unsecure network wherein the receiving completes a first hop and the proxy is an ending point of a first communication associated with the first hop; decrypting the encrypted data into decrypted data; examining the decrypted data for security purposes; re-encrypting the examined decrypted data; and sending the re-encrypted data from the proxy to an origin server over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop."

While Perlman describes the examination of data for security purposes, Perlman does not describe the use of a proxy, as is claimed. A full-text search of Perlman fails to show the existence of any instance of the word "proxy," and an examination of the teachings of Perlman fails to demonstrate that elements of Perlman act as a proxy by terminating or acting as an ending point for one communication and starting or acting as a starting point for any other communication, as is claimed. This omission is a major difference between the claimed invention and the techniques described by Perlman.

Instead of describing a proxy, Perlman describes a content screening mechanism that has the ability to decrypt and examine the contents of an encrypted communication. The content screener, and the firewall in which the content screener is sometimes (although not always) implemented, perform no proxying functions. For example, as far as the client in Perlman is concerned, a communication occurs between the client and the server, not between the client and the firewall. Similarly, from the perspective of the server in Perlman, the communication is received from the client, not from the firewall. In fact, in some implementations described by Perlman, including those described with reference to FIG. 6, the firewall is completely optional. In contrast, in the claimed invention, the communication is always conducted through an intermediary proxy. From the perspective of the client, the communication occurs between the client and the proxy. Similarly, from the perspective of the server, the communication occurs between the proxy and the server. The client cannot communicate with the server directly and the server cannot communicate with the client directly – all communications are terminated at the proxy.

Because the proxy is always the ending point of the communication from the client and a starting point of another communication to the server, there can be no "end-to-end encryption," in the sense that the server decrypts the same encrypted message originally sent by the client, as is described by Perlman. Indeed, even in the cases where the claimed second communication, between the proxy and the server, is described as being encrypted, the data is encrypted by the proxy, not by the client.

At least for these reasons, claim 1 is allowable and the rejection thereof should be withdrawn.

Claims 4-10 and 12-13

Claims 4-10 and 12-13 depend from claim 1 and are allowable at least by virtue of this dependency. Accordingly, the rejections of these claims should be withdrawn.

Claims 28-30

Claim 28, as amended, recites "a system comprising: a client to send encrypted data over an unsecure network and be a starting point of a first hop; a proxy within a secure network to receive the encrypted data, decrypt the encrypted data into decrypted data, perform a test relative to the decrypted data, and send the decrypted data over the secure network in response to the test yielding a particular response wherein the proxy is an ending point of a first communication associated with the first hop and a starting point of a second communication associated with a second hop; and, an origin server within the secure network to receive the decrypted data and be an ending point of the second communication associated with the second hop."

Similar to the discussion presented previously with respect to claim 1, Perlman fails to show the use of a proxy, as is claimed. At least for this reason, claim 28 is allowable and the rejection thereof should be withdrawn.

Claims 29-30 depend from claim 28 and are allowable at least by virtue of this dependency. Accordingly, the rejections of these claims should be withdrawn.

<u>Claims 33-36</u>

Claim 33, as amended, recites "a proxy comprising: one or more communication components enabling the proxy to communicate over a first network and a second network; a processor; and, a computer-readable medium having a computer program stored thereon for execution by the processor to: receive data that is originally encrypted or unencrypted from a client over the first network as part of a first hop wherein the proxy is an ending point of a first communication associated with the first hop, decrypt the data where the data was originally encrypted, perform a test relative to the data, in response to the test yielding a particular result, send the data as part of a second hop unencrypted to an origin server over the second network where the data was originally encrypted, or send the data as part of the second hop unencrypted or encrypted to the origin server over the second network where the data was originally unencrypted wherein the proxy is a starting point of a second communication associated with the second hop."

Similar to the discussion presented previously with respect to claim 1, Perlman fails to show the use of a proxy, as is claimed. At least for this reason, claim 33 is allowable and the rejection thereof should be withdrawn.

Claims 34-36 depend from claim 33 and are allowable at least by virtue of this dependency. Accordingly, the rejections of these claims should be withdrawn.

Claim 14

Claim 14 recites "a proxy method comprising: receiving unencrypted data from a client over a secure network; examining the unencrypted data for security purposes; and, in response to the examining yielding that the unencrypted data does not present a security risk: encrypting the unencrypted data into encrypted data; sending the encrypted data to an origin server over an unsecure network."

Perlman does not show multiple elements of claim 14. For example, claim 14 includes the limitation of "receiving unencrypted data from a client over a secure network." The Office Action cites column 4, lines 32-37, of Perlman as anticipating this limitation. However, this section of Perlman, and the remainder of Perlman, describes only the receiving of encrypted data (not unencrypted data) from a client over an unsecure (not secure) network. That is, Perlman describes the situation of, for example, receiving encrypted data from a client over an unsecure network, like the Internet. In contrast, this element of claim 14 describes the receiving of unencrypted data from a client over a secure network. One described example of a situation in which the type of receiving described in claim 14 might occur is a case where the client is a device like a wireless phone on a secure network maintained by a wireless carrier. Because the exemplary wireless carrier network is secure, the communication from the client may be transmitted unencrypted, as is claimed.

Similarly, claim 14 includes the limitation of "sending the encrypted data to an origin server over an unsecure network." The Office Action cites a variety of blocks in the figures of Perlman as well as a number of lines of the specification of Perlman in support of this rejection. However, the specifically cited sections of Perlman, and the remainder of Perlman, do not describe the sending of encrypted data to a server over an unsecure network – instead, Perlman describes the sending of decrypted data produced by a content screener to a server over a secure network.

While elements of claim 14 may appear similar to the teachings of Perlman, it may be appreciated that they are in fact different when one considers the functionality enabled by a method like that described with respect to claim 14. For example, consider again the previous example where the client is a wireless phone and the initial unencrypted data travels over a secure wireless carrier network, and where an intermediary proxy encrypts the data for transmission over an unsecure network like the Internet. In this example, the proxy can enable secure communication with sites on the Internet that support protocols like SSL, even when the original client – the wireless phone in this example – doesn't support a protocol like SSL. Such a system is not taught or contemplated by Perlman.

At least for these reasons, claim 14 is allowable and the rejection thereof should be withdrawn.

<u>Claims 16-24 and 26-27</u>

Claims 16-24 and 26-27 depend from claim 14 and are allowable at least by virtue of this dependency. Accordingly, the rejections of these claims should be withdrawn.

<u>Claims 31-32</u>

Claim 31 recites "a system comprising: a client to send unencrypted data over a secure network; a proxy within the secure network to receive the unencrypted data,

perform a test relative to the unencrypted data, encrypt the unencrypted data into encrypted data, and send the encrypted data over an unsecure network in response to the test yielding a particular response; and, an origin server to receive the encrypted data."

Similar to the discussion presented previously with respect to claim 14, Perlman fails to show the sending, from a client, of unencrypted data over a secure network, or the sending, to a server, of encrypted data over an unsecure network, as is claimed. In addition, similar to the discussion presented previously with respect to claim 1, Perlman fails to show a proxy, as is claimed. At least for these reasons, claim 31 is allowable and the rejection thereof should be withdrawn.

Claim 32 depends from claim 31 and is allowable at least by virtue of this dependency. Accordingly, the rejection of this claim should be withdrawn.

CONCLUSION

Accordingly, in view of the above amendment and remarks it is submitted that the claims are patentably distinct over the prior art and that all the rejections and objections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested. Based on the foregoing, Applicant respectfully requests that the pending claims be allowed, and that a timely Notice of Allowance be issued in this case. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's agent at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an enclosed check please charge any deficiency to Deposit Account No. 50-0463.

Respectfully submitted,
Microsoft Corporation

Date: June 23, 2006	By: Andrew D. Enfield
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399	Andrew D. Enfield, Reg. No.: 57,651 Agent for Applicants Direct telephone (425) 703-8227
	James R. Banowsky, Reg. No.: 37,773

CERTIFICATE OF MAILING OR TRANSMISSION
(Under 37 CFR § 1.8(a)) or ELECTRONIC FILING

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

June 23, 2006 Date	Noemi Tovar Signature
	Noemi Tovar Printed Name